# Digital signatur verification and program transmission

Patent Number: US2002116619
Publication date: 2002-08-22
Inventor(s): URAMOTO NAOHIKO (JP); MARUYAMA HIROSHI (JP)
Applicant(s): IBM (US)
Requested Patent: JP2002164884
Application Number: US20010017926 20011029
Priority Number(s): JP20000336586 20001102
IPC Classification: H04L9/00
EC Classification: H04L9/32S
Equivalents:

## Abstract

The invention includes a proxy server that constitutes means for providing, verifying and logging a digital signature for a message that is to be exchanged via a network, so that a security function for a digital signature can be implemented without changing an application program. In an example embodiment, a digital signature system comprises: applications for performing data processing; and a signature server connected to the applications via a LAN, wherein the signature server intercepts the message communication from the application to a destination device outside the LAN, provides a digital signature for a message document to be exchanged through communication, and transmits the obtained message document to the destination device

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－164884
（P2002－164884A）
(43)公開日　平成14年６月７日(2002.6.7)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/32 | | Ｇ０６Ｆ　17/60 | ５１２ | ５Ｊ１０４ |
| Ｇ０６Ｆ　17/60 | ５１２ | Ｇ０９Ｃ　1/00 | ６４０Ｂ | |
| Ｇ０９Ｃ　1/00 | ６４０ | Ｈ０４Ｌ　9/00 | ６７５Ｄ | |
| Ｈ０４Ｌ　9/08 | | | ６０１Ｃ | |

審査請求　有　請求項の数20　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－336586(P2000－336586)

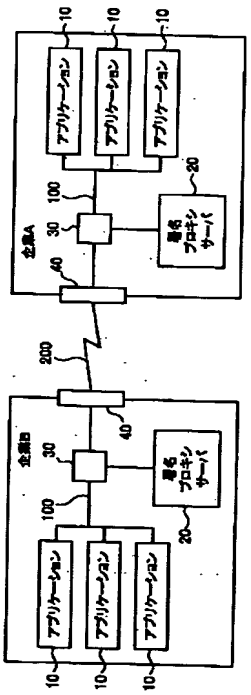
(22)出願日　平成12年11月２日(2000.11.2)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(74)代理人　100086243
弁理士　坂口　博　（外４名）

最終頁に続く

(54)【発明の名称】　プロキシサーバ、電子署名システム、電子署名検証システム、ネットワークシステム、電子署名方法、電子署名検証方法、記憶媒体及びプログラム伝送装置

(57)【要約】
【課題】　ネットワークを介して送受されるメッセージの電子署名、検証、ロギングを行う手段をプロキシサーバの形で実装することにより、アプリケーション・プログラムの変更を必要とせずに、電子署名によるセキュリティ機能を実現する。
【解決手段】　データ処理を行うアプリケーション１０と、ＬＡＮ１００を介してこのアプリケーション１０に接続された署名プロキシサーバ２０とを備え、この署名プロキシサーバ２０は、アプリケーション１０からＬＡＮ１００の外部の装置へのメッセージ通信をインターセプトし、このメッセージ通信におけるメッセージ文書に電子署名を行い、電子署名付きメッセージ文書を送信先である装置へ送信する。



【特許請求の範囲】
【請求項１】　アプリケーション間で行われる通信を中継し、付加的処理を行うプロキシサーバにおいて、
前記アプリケーション間でやりとりされるメッセージ文書に施す電子署名を生成するための鍵を管理する鍵管理部と、
所定の前記アプリケーションから送信されたメッセージ文書を取得し、当該メッセージ文書に基づいて電子署名を行うための鍵を決定する署名鍵判定部と、
前記署名鍵判定部の決定に基づいて前記鍵管理部から取得した鍵を用いて、前記メッセージ文書に対して電子署名を行い、署名された当該メッセージ文書を送信先である他の前記アプリケーションに送る署名生成部とを備えたことを特徴とするプロキシサーバ。
【請求項２】　前記鍵管理部は、前記鍵の取得条件を設定し、当該取得条件を満足する場合に、前記署名生成部が該当する前記鍵を取得可能とすることを特徴とする請求項１に記載のプロキシサーバ。
【請求項３】　前記署名生成部は、前記メッセージ文書に施す電子署名を生成するための鍵を取得できない場合に、予め設定された代替用の鍵を用いて電子署名を行うことを特徴とする請求項２に記載のプロキシサーバ。
【請求項４】　前記署名生成部は、代替用の鍵を用いて前記メッセージ文書に対する電子署名を行った後、当該メッセージ文書に基づいて決定された本来の鍵の取得条件が満たされて当該本来の鍵を取得可能となった場合に、当該本来の鍵を用いて当該メッセージ文書に対して改めて電子署名を行うことを特徴とする請求項３に記載のプロキシサーバ。
【請求項５】　前記署名生成部により電子署名が施された前記メッセージ文書を格納し、ログを管理するログ管理部をさらに備えることを特徴とする請求項１に記載のプロキシサーバ。
【請求項６】　前記ログ管理部は、前記署名生成部が前記代替用の鍵を用いて電子署名を行った場合に、電子署名が施された前記メッセージ文書と共に、電子署名が施される前の前記メッセージ文書を格納し、
前記署名生成部は、前記本来の鍵を用いて電子署名を行う場合に、前記ログ管理部から前記電子署名が施される前のメッセージ文書を取得して電子署名を行うことを特徴とする請求項４に記載のプロキシサーバ。
【請求項７】　データ処理を行うアプリケーションと、ネットワークを介して当該アプリケーションに接続されたプロキシサーバとを備え、
前記プロキシサーバは、前記アプリケーションから前記ネットワーク外部の装置へのメッセージ通信をインターセプトし、当該メッセージ通信におけるメッセージ文書に電子署名を行い、電子署名付きメッセージ文書を前記装置へ送信することを特徴とする電子署名システム。
【請求項８】　前記プロキシサーバは、
メッセージ文書の内容に応じて電子署名を行うための鍵を変更可能とすると共に、
前記鍵に対して使用条件を設定し、当該使用条件を満足する場合に当該鍵を用いた電子署名を実行可能とすることを特徴とする請求項７に記載の電子署名システム。
【請求項９】　前記プロキシサーバは、
前記メッセージ文書に電子署名を施すための前記鍵に関する前記使用条件が満たされていない場合に、予め設定された代替用の鍵を用いて電子署名を行い、
前記代替用の鍵を用いた電子署名を行った後に本来の前記鍵に関する使用条件が満たされたならば、当該本来の鍵を用いて前記メッセージ文書に対して改めて電子署名を行うことを特徴とする請求項８に記載の電子署名システム。
【請求項１０】　データ処理を行うアプリケーションと、ネットワークを介して当該アプリケーションに接続されたプロキシサーバとを備え、
前記プロキシサーバは、前記ネットワーク外部の装置から前記アプリケーションへのメッセージ通信をインターセプトし、当該メッセージ通信におけるメッセージ文書の電子署名を検証し、当該検証により正当性が確認された当該メッセージ文書を前記アプリケーションへ送信することを特徴とする電子署名検証システム。
【請求項１１】　広域ネットワークで接続された複数のグループを備え、各グループは、データ処理を行うアプリケーションと、ローカルなネットワークを介して当該アプリケーションに接続されたプロキシサーバとを備えたネットワークシステムにおいて、
前記プロキシサーバは、
自グループの前記アプリケーションから他のグループの前記アプリケーションへのメッセージ通信をインターセプトし、当該メッセージ通信におけるメッセージ文書に電子署名を行い、電子署名付きメッセージ文書を前記他のグループの前記アプリケーションへ送信し、
他のグループの前記アプリケーションから自グループの前記アプリケーションへのメッセージ通信をインターセプトし、当該メッセージ通信におけるメッセージ文書の電子署名を検証し、当該検証により正当性が確認された当該メッセージ文書を前記自グループのアプリケーションへ送信することを特徴とするネットワークシステム。
【請求項１２】　前記プロキシサーバは、
自グループの前記アプリケーションがメッセージ文書を送信する場合に、前記電子署名付きメッセージ文書を保管してログ管理を行い、
他のグループからメッセージ文書を受信した場合に、前記電子署名の検証により正当性が確認された当該メッセージ文書を保管してログ管理を行い、
所定のタイミングで、同一のメッセージ文書に関する送信側のログと受信側のログとを比較し、メッセージ通信の正当性を確認することを特徴とする請求項１１に記載

のネットワークシステム。
【請求項１３】　前記プロキシサーバは、同一のメッセージ文書に関する電子署名の署名情報を比較することを特徴とする請求項１２に記載のネットワークシステム。
【請求項１４】　前記プロキシサーバは、同一のメッセージ文書に関する電子署名を行うために用いられるハッシュ値を比較することを特徴とする請求項１２に記載のネットワークシステム。
【請求項１５】　アプリケーション間で行われる通信におけるメッセージ文書に電子署名を施すことにより、当該メッセージ文書の正当性を保証する電子署名方法において、
所定の前記アプリケーションから送信されたメッセージ文書の種類に応じて、当該メッセージ文書に電子署名を施すための鍵を選択するステップと、
当該鍵に対して使用条件が設定されている場合であって、当該使用条件が満たされていない場合に、当該鍵に代えて予め設定された代替用の鍵を用いて前記メッセージ文書に電子署名を行い、当該電子署名付きのメッセージ文書を前記アプリケーションから送信された際の送信先に送信するステップと、
前記代替用の鍵を用いて前記メッセージ文書に電子署名を行った後、本来の前記鍵における前記使用条件が満たされた際に、当該本来の鍵を用いて前記メッセージ文書に改めて電子署名を行い、当該電子署名付きのメッセージ文書を前記アプリケーションから送信された際の送信先に送信するステップとを含むことを特徴とする電子署名方法。
【請求項１６】　アプリケーション間で行われる通信におけるメッセージ文書に施された電子署名を検証することにより、当該メッセージ文書の正当性を確認する電子署名検証方法において、
受信したメッセージ文書に施された電子署名が、当該メッセージ文書の種類に応じて定められた鍵ではなく、当該鍵の代替用の鍵を用いて行われた電子署名である場合に、当該代替用の鍵を用いて署名された当該メッセージ文書を受領するステップと、
前記代替用の鍵を用いて署名されたメッセージ文書を受領した後、本来の前記鍵を用いて署名された当該メッセージ文書を受信するステップと、
前記本来の鍵を用いた電子署名を検証することにより、先に受領した前記代替用の鍵を用いて署名されたメッセージ文書の正当性を確認するステップとを含むことを特徴とする電子署名検証方法。
【請求項１７】　コンピュータに実行させるプログラムを当該コンピュータの入力手段が読取可能に記憶した記憶媒体において、
前記プログラムは前記コンピュータをアプリケーション間でやりとりされるメッセージ文書に施す電子署名を生成するための鍵を管理する鍵管理手段と、
所定の前記アプリケーションから送信されたメッセージ文書を取得し、当該メッセージ文書に基づいて電子署名を行うための鍵を決定する署名鍵判定手段と、
前記署名鍵判定手段の決定に基づいて前記鍵管理手段から取得した鍵を用いて、前記メッセージ文書に対して電子署名を行う署名生成手段として機能させることを特徴とする記憶媒体。
【請求項１８】　コンピュータに実行させるプログラムを当該コンピュータの入力手段が読取可能に記憶した記憶媒体において、
前記プログラムは、
所定のアプリケーションから送信されたメッセージ文書の種類に応じて、当該メッセージ文書に電子署名を施すための鍵を選択する処理と、
原則として選択された前記鍵を用いて前記メッセージ文書に電子署名を行い、当該鍵に対して使用条件が設定されている場合であって、当該使用条件が満たされていない場合に、当該鍵に代えて予め設定された代替用の鍵を用いて前記メッセージ文書に電子署名を行う処理と、
前記代替用の鍵を用いて前記メッセージ文書に電子署名を行った後、本来の前記鍵における前記使用条件が満たされた際に、当該本来の鍵を用いて前記メッセージ文書に改めて電子署名を行う処理とを前記コンピュータに実行させることを特徴とする記憶媒体。
【請求項１９】　コンピュータを、アプリケーション間でやりとりされるメッセージ文書に施す電子署名を生成するための鍵を管理する鍵管理手段と、所定の前記アプリケーションから送信されたメッセージ文書を取得し、当該メッセージ文書に基づいて電子署名を行うための鍵を決定する署名鍵判定手段と、前記署名鍵判定手段の決定に基づいて前記鍵管理手段から取得した鍵を用いて、前記メッセージ文書に対して電子署名を行う署名生成手段として機能させるプログラムを記憶する記憶手段と、前記記憶手段から前記プログラムを読み出して当該プログラムを送信する送信手段とを備えたことを特徴とするプログラム伝送装置。
【請求項２０】　コンピュータに、
所定のアプリケーションから送信されたメッセージ文書の種類に応じて、当該メッセージ文書に電子署名を施すための鍵を選択する処理と、原則として選択された前記鍵を用いて前記メッセージ文書に電子署名を行い、当該鍵に対して使用条件が設定されている場合であって、当該使用条件が満たされていない場合に、当該鍵に代えて予め設定された代替用の鍵を用いて前記メッセージ文書に電子署名を行う処理と、前記代替用の鍵を用いて前記メッセージ文書に電子署名を行った後、本来の前記鍵における前記使用条件が満たされた際に、当該本来の鍵を用いて前記メッセージ文書に改めて電子署名を行う処理とを実行させるプログラムを記憶する記憶手段と、
前記記憶手段から前記プログラムを読み出して当該プロ

グラムを送信する送信手段とを備えたことを特徴とするプログラム伝送装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットなどにおけるビジネス間メッセージ通信において、電子署名と検証を行うことによりメッセージの認証と証拠性を保証する技術に関する。

【０００２】

【従来の技術】近年、インターネットなどのネットワーク技術の進歩により、ネットワークを介したメッセージ通信により商取引や業務を行う事業形態が普及してきている。このような事業形態においては、セキュリティの確保は大きな課題である。

【０００３】ネットワーク上のビジネス間メッセージ通信におけるデータ交換フォーマットとして、ＸＭＬ電子署名が定義されつつあり、このＸＭＬ電子署名によりメッセージ認証及びトランザクションの証拠性を確保することが期待されている。ここで、電子署名とは、デジタル情報に署名情報（署名情報自体もデジタル情報）を付加して、文書の正当性を保証する技術である。一般に、署名には公開鍵暗号が用いられる。署名者はハッシュ関数で圧縮された文書と自分だけが知っている秘密鍵を用いて署名文を作り、元の文書と一緒に送る。検証者は署名者の公開鍵と署名文と元の文書とに基づいて署名が正しいかどうかを検査する。

【０００４】電子署名は、第三者や受取人(検証者)によって偽造できない機能と、署名を行った本人が後でそれを否認できない機能を持つ。したがって、各々のメッセージを一意性のあるＩＤ番号と共に署名することにより、

１．メッセージが確かに発信者によって作成されたこと

２．メッセージが改ざんされていないこと

３．同一のメッセージを間違って２度受け付けないこと

４．発信者がメッセージを発信したこと

のそれぞれを証明する機能を実現することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、既存の暗号ライブラリを用いてメッセージの署名、検証を行うためには、この電子署名を利用しようとするアプリケーション・プログラムに変更を加えなければならず、そのために要するコストが大きい。

【０００６】また、電子署名の証拠性を高めるため、電子署名を行うための条件を設定する場合がある。例えば、一定の時間帯にのみ署名することができる時間制約のある電子署名や、一定の処理を行わなければ署名することができない電子署名などが考えられる。このような場合、当該電子署名の代用として他の電子署名を用い、後で当該電子署名により事後署名を行うことができれば、業務上、便利な場合がある。

【０００７】また、署名及び検証を行うと同時に、事後の監査を可能にするために、これらの署名付きメッセージを安全なログに格納しなければならない。これら格納されたメッセージは、署名が付いているので改ざんはできないが、そのままでは閲覧することは可能である。しかし、ビジネス間のメッセージ通信においては、重要な秘密情報が含まれている可能性もあるので、ログに対しては、アクセスコントロールが必要である。

【０００８】そこで、本発明は、ネットワークを介して送受されるメッセージの電子署名、検証、ロギングを行う手段をプロキシサーバの形で実装することにより、アプリケーション・プログラムの変更を必要とせずに、電子署名によるセキュリティ機能を実現することを目的とする。

【０００９】また、本発明は、プロキシサーバを用いて電子署名及び検証を制御することにより、事後署名のような署名方法を実現することを他の目的とする。

【００１０】また、本発明は、プロキシサーバを用いてメッセージのロギングを行うことにより、メッセージのログに対するアクセス制御を可能とすることをさらに他の目的とする。

【００１１】

【課題を解決するための手段】上記の目的を達成するため、本発明は、アプリケーション間で行われる通信を中継し、付加的処理を行うプロキシサーバにおいて、アプリケーション間でやりとりされるメッセージ文書に施す電子署名を生成するための鍵を管理する鍵管理部と、所定のアプリケーションから送信されたメッセージ文書を取得し、このメッセージ文書に基づいて電子署名を行うための鍵を決定する署名鍵判定部と、この署名鍵判定部の決定に基づいてこの鍵管理部から取得した鍵を用いて、このメッセージ文書に対して電子署名を行い、署名されたメッセージ文書を送信先である他のアプリケーションに送る署名生成部とを備えたことを特徴とする。これにより、メッセージ文書の内容に応じて、異なるセキュリティを持った電子署名を行うことができる。

【００１２】ここで、この鍵管理部は、この鍵の取得条件を設定し、この取得条件を満足する場合にのみ、署名生成部が該当する鍵を取得可能とすることができる。すなわち、鍵を取得するために一定の条件を満足することを必要とするため、この鍵を用いた電子署名の信頼性を高めることができる。取得条件としては、鍵を使用できる時間帯を制限する時間条件や、メッセージ文書に対して一定の処理が行われた後でなければ鍵を使用できないとする処理条件を設定することができる。

【００１３】また、この署名生成部は、メッセージ文書に施す電子署名を生成するための鍵に関して取得条件を満足していないために、この鍵を取得できない場合、予め設定された代替鍵を用いて電子署名を行うことができる。この場合、署名生成部は、代替鍵を用いて電子署名

を行った後、署名対象であるメッセージ文書に基づいて決定された本来の鍵の取得条件が満たされて、この本来の鍵を取得可能となった場合に、この本来の鍵を用いて改めて電子署名を行うことができる。この事後的な署名は、代替鍵を用いて署名されたメッセージ文書に対して追加的に行っても良いし、代替鍵を用いた署名を行う前の状態のメッセージ文書に対して新規に行っても良い。

【００１４】さらに、本発明のプロキシサーバは、上記の構成に加えて、署名生成部により電子署名が施されたメッセージ文書を格納し、ログを管理するログ管理部を備える構成とすることができる。上述したように、代替鍵を用いた署名を行う前の状態のメッセージ文書に対して新規に事後署名を行う場合、このログ管理部は、署名生成部が代替鍵を用いて電子署名を行った場合に、電子署名が施されたメッセージ文書と共に、電子署名が施される前のメッセージ文書を格納し、署名生成部は、本来の鍵を用いて電子署名を行う場合に、このログ管理部から電子署名が施される前の状態のメッセージ文書を取得して電子署名を行うことができる。

【００１５】また、本発明は、上述したプロキシサーバを用い、次のように構成されたことを特徴とする電子署名システムを提供することができる。すなわち、この電子署名システムは、データ処理を行うアプリケーションと、ネットワークを介してこのアプリケーションに接続されたプロキシサーバとを備え、このプロキシサーバは、アプリケーションからネットワーク外部の装置へのメッセージ通信をインターセプトし、このメッセージ通信におけるメッセージ文書に電子署名を行い、電子署名付きメッセージ文書を送信先である装置へ送信する。

【００１６】この電子署名システムにおいて、このプロキシサーバは、ネットワーク上を流れる情報を（受け手及び送り手が透過に気づかれずに）インターセプトするハードウエア、または同様な機能を実現するソフトウェアにて実現されるスイッチを介して前記ネットワークに接続する。このようなスイッチとしては、レイヤー４スイッチを用いることができる。これにより、アプリケーションによるメッセージ通信をインターセプトできるため、アプリケーションに何ら変更を加えることなく（すなわち、アプリケーションは電子署名を全く意識せずに）メッセージ文書に電子署名を行うことができることとなる。

【００１７】また、本発明は、次のように構成されたことを特徴とする電子署名検証システムを提供することができる。すなわち、この電子署名検証システムは、データ処理を行うアプリケーションと、ネットワークを介してこのアプリケーションに接続されたプロキシサーバとを備え、このプロキシサーバは、ネットワーク外部の装置からアプリケーションへのメッセージ通信をインターセプトし、このメッセージ通信におけるメッセージ文書の電子署名を検証し、この検証により正当性が確認されたメッセージ文書をアプリケーションへ送信する。

【００１８】この電子署名検証システムにおいても、このプロキシサーバは、レイヤー４スイッチなどのスイッチを介して前記ネットワークに接続することができる。これにより、ネットワーク外部からのメッセージ通信をインターセプトできるため、アプリケーションに何ら変更を加えることなく（すなわち、アプリケーションは電子署名を全く意識せずに）メッセージ文書の電子署名を検証することができることとなる。

【００１９】さらに本発明は、広域ネットワークで接続された複数のグループを備え、各グループは、データ処理を行うアプリケーションと、ローカルなネットワークを介して当該アプリケーションに接続されたプロキシサーバとを備えたネットワークシステムにおいて、このプロキシサーバは、自グループのアプリケーションから他のグループのアプリケーションへのメッセージ通信をインターセプトし、このメッセージ通信におけるメッセージ文書に電子署名を行い、電子署名付きメッセージ文書を送信先である他のグループのアプリケーションへ送信し、他のグループのアプリケーションから自グループのアプリケーションへのメッセージ通信をインターセプトし、このメッセージ通信におけるメッセージ文書の電子署名を検証し、この検証により正当性が確認されたメッセージ文書を送信先である自グループのアプリケーションへ送信することを特徴とする。

【００２０】ここで、このプロキシサーバは、自グループのアプリケーションがメッセージ文書を送信する場合に、電子署名付きメッセージ文書を保管してログ管理を行い、かつ他のグループからメッセージ文書を受信した場合に、電子署名の検証により正当性が確認されたメッセージ文書を保管してログ管理を行う。そして、所定のタイミングで、同一のメッセージ文書に関する送信側のログと受信側のログとを比較することにより、メッセージ通信の正当性を確認することができる。比較する情報は、ログの全情報である必要はなく、同一のメッセージ文書に関する電子署名の署名情報や、同一のメッセージ文書に関する電子署名を行うために用いられるハッシュ値を比較することが可能である。この場合、ログにおけるこれらの情報が同一であれば、メッセージ通信の正当性が確認できる。そして、これらの情報が相違している場合、改めてログの全情報を比較することにより、詳細な検討を行うこととなる。

【００２１】また、本発明は、アプリケーション間で行われる通信におけるメッセージ文書に電子署名を施すことにより、このメッセージ文書の正当性を保証する電子署名方法において、所定のアプリケーションから送信されたメッセージ文書の種類に応じて、このメッセージ文書に電子署名を施すための鍵を選択するステップと、この鍵に対して使用条件が設定されている場合であって、この使用条件が満たされていない場合に、この鍵に代え

て予め設定された代替鍵を用いてメッセージ文書に電子署名を行い、電子署名付きのメッセージ文書をアプリケーションから送信された際の送信先に送信するステップと、この代替鍵を用いて電子署名を行った後、本来の鍵における使用条件が満たされた際に、この本来の鍵を用いて改めて電子署名を行い、電子署名付きのメッセージ文書を送信先に送信するステップとを含む構成とする。

【００２２】さらに本発明は、アプリケーション間で行われる通信におけるメッセージ文書に施された電子署名を検証することにより、このメッセージ文書の正当性を確認する電子署名検証方法において、受信したメッセージ文書に施された電子署名が、このメッセージ文書の種類に応じて定められた鍵ではなく、代替鍵を用いて行われた電子署名である場合に、この代替鍵を用いて署名されたこのメッセージ文書を受領するステップと、代替鍵を用いて署名されたメッセージ文書を受領した後、本来の鍵を用いて署名されたメッセージ文書を受信するステップと、本来の鍵を用いた電子署名を検証することにより、先に受領した代替鍵を用いて署名されたメッセージ文書の正当性を確認するステップとを含むことを特徴とする。

【００２３】また、本発明は、これらの電子署名方法や電子署名検証方法の各ステップに相当する処理をコンピュータに実行させるプログラム、あるいは、コンピュータを制御して上述したプロキシサーバを実現するプログラム・プロダクトとして作成し、このプログラムを記憶した記憶媒体やこのプログラムを伝送する伝送装置として提供することができる。

【００２４】

【発明の実施の形態】以下、添付図面に示す実施の形態に基づいて、この発明を詳細に説明する。図１は、本実施の形態における電子署名システムの全体構成を説明する図である。図１において、企業Ａと企業Ｂとは、メッセージ通信を行うアプリケーション１０群と、アプリケーション１０群によってやりとりされるメッセージにおける電子署名を管理する署名プロキシサーバ２０とを備える。ここで、アプリケーション１０は、所定のプログラムによって制御され、メッセージ通信を含む種々の機能を実現するコンピュータ装置である。図１においては、各アプリケーション１０及び署名プロキシサーバ２０は別個に記載されているが、これは機能に基づく区別であり、必ずしもハードウェアの構成を意味しない。すなわち、物理的に個別のハードウェアにて構成されても良いし、いくつかのアプリケーション１０が共通のハードウェア上で動作していても良い。

【００２５】図１に示すように、企業Ａ、Ｂはインターネットなどの広域なネットワーク２００を介して接続されている。また、企業Ａ、Ｂのそれぞれにおいて、アプリケーション１０は、社内ネットワークなどのＬＡＮ１００に接続され、ファイヤーウォール４０を経てネットワーク２００に接続されている。署名プロキシサーバ２０は、スイッチ３０を介してＬＡＮ１００に接続されている。ここで、スイッチ３０は、ネットワーク上を流れる情報を（受け手及び送り手が透過に気づかれずに）インターセプトするハードウエア（例えばレイヤー４スイッチなど）、または同様な機能を実現するソフトウェアにて実現される。

【００２６】なお、本実施の形態では、ビジネス間通信を想定し、企業Ａ、Ｂ間のメッセージのやりとりにおいて電子署名システムを用いる例について説明するが、ビジネスに関わらず、特定のグループどうしのメッセージ通信や、個人レベルを含む電子メールのやりとりにおいても、本実施の形態による電子署名システムを適用することができる。

【００２７】また、図１に示す構成は例示に過ぎず、アプリケーション１０及び署名プロキシサーバ２０を一つのグループとし、複数のグループどうしをネットワークを介して接続する構成であれば、他の構成であっても良い。したがって、スイッチ３０及びファイヤーウォール４０は、必ずしも必須の構成要件ではない。ただし、本実施の形態では、企業間通信を考慮してファイヤーウォール４０を備えるものとする。また、アプリケーション１０を変更することなくアプリケーション１０間の通信をインターセプトして電子署名の付加及び管理を行うために、スイッチ３０を介して署名プロキシサーバ２０を接続する構成を取るものとする。

【００２８】さらにまた、本実施の形態において、企業Ａ、Ｂ間（または企業Ａ、Ｂのアプリケーション１０間）におけるメッセージ通信はＸＭＬ文書によるものとする。ただし、本実施の形態をＸＭＬ以外の他の形式による文書や電子メールに対してもそのまま適用できることは言うまでもない。

【００２９】図１において、アプリケーション１０は、商品の発注書や受注書、明細書など、業務において必要となるメッセージ文書をＸＭＬ文書として作成し、相手企業の業務上対応するアプリケーション１０に対して送信する。

【００３０】署名プロキシサーバ２０は、社内のアプリケーション１０から他社へのメッセージ文書送信のためのＨＴＴＰ接続をインターセプトする機能と、反対に社外から社内の所定のアプリケーション１０へのＨＴＴＰ接続をインターセプトする機能（リバースプロキシ）とを備える。そして、インターセプトしたメッセージ文書に関して、社内から社外へ送信される文書については、必要な電子署名を行い、社外から社内へ送信された文書については、電子署名の検証を行う。署名プロキシサーバ２０の詳細な構成及び動作については後述する。

【００３１】ＬＡＮ１００とネットワーク２００との境界（出入口）に置かれたファイヤーウォール４０と各アプリケーション１０との間にスイッチ３０を設け、この

スイッチ30を介して署名プロキシサーバ20とLAN100とを接続することにより、署名プロキシサーバ20が上記のHTTP接続をインターセプトすることができる。なお、スイッチ30を用いず、各アプリケーション10のURLを変更することにより、署名プロキシサーバ20を経由して通信を行うように設定することもできる。しかし、スイッチ30を用いることにより、アプリケーション10に対して何ら変更を行うことなく、署名プロキシサーバ20による電子署名の付加及び管理を行うことができる。

【0032】また、署名プロキシのプラットフォーム（OS）は、次の各点で高いセキュリティを要求される。すなわち、

1．署名を行うための秘密鍵は盗まれてはならないこと

2．検証を行うためのルート認証局の鍵は、書き換えられてはならないこと

3．ログのアクセスコントロールをバイパスされてはならないこと

である。このため、署名プロキシサーバ20に対しては、通常のインターネットアクセスができない、もしくは非常に限られたものにする必要がある。そのための方法として、例えば、プロキシに対して外部からアクセスできないネットワークアドレス（例えば、192.168.xx.xxというようなローカルアドレス）を用いる方法が考えられる。また、別の方法として、インターセプトしたパケットを、一度、RS-232CやUSBなど、通常はTCP/IPを通さないメディアに変換し、その後に署名プロキシサーバ20に送る方法がある。これらの方法を用いることにより、より安全に鍵やログを守ることができる。

【0033】図2は、署名プロキシサーバ20の電子署名の付加に関する構成を示す図である。なお、本実施の形態における電子署名は、ハッシュ関数を用いた公開鍵暗号によるXML電子署名とする。図2を参照すると、署名プロキシサーバ20は、電子署名を行うために署名用の秘密鍵を選択する署名鍵判定部21と、署名用の秘密鍵を管理する鍵管理部22と、署名鍵判定部21の選択にしたがって鍵管理部22から必要な秘密鍵を取得する署名鍵取得部23と、署名鍵取得部23により取得された秘密鍵を用いて署名情報を生成し、メッセージ文書に署名する署名生成部24と、メッセージ文書のログを管理するログ管理部25とを備える。

【0034】署名鍵判定部21は、社内のアプリケーション10から送信されたメッセージ文書であるXML文書を取得する。そして、所定の鍵選択ルールに基づいて、当該XML文書に対して適切な署名を行うために必要な秘密鍵を選択する。ここで、鍵選択ルールには、XML文書の内容に基づいて秘密鍵を選択するための規則であり、例えばXML形式で記述されている。なお、XML文書に付加される電子署名には、社外への文書にすべて自動的に付加される日付印のようなものや、責任権限のある担当者が1件ずつチェックして署名を行うもの、会社の公印のようなもの、あるいはこれらの中間的な性格を持つものなど、種々の意味を設定することができる。これら署名の意味の違いは、署名鍵の意味付け（通常、署名鍵に対応するデジタル証明書の中に、認証プラクティスステートメントとして記述されている）によって決定される。上述したように、XML文書の内容に応じて異なる秘密鍵を用いることができるが、これは、署名鍵判定部21において、XML文書の内容と用いる秘密鍵との組を規則として登録することによって実現できる。XML文書の内容は、XPathを用いて表現されるので、複雑なパターンを指定することができる。さらに、これを利用して、XML文書中の特定の範囲のみを署名範囲として指定することもできる。図6は、XML形式で記述された鍵選択ルールの例を示す図である。ここでは、電子商取引において、100万円以上の額の取引には、電子署名を行うための秘密鍵として会社印（に相当する秘密鍵）を使用し、10万円以上の額の取引には、担当者印（に相当する秘密鍵）を使用することが規定されている。

【0035】鍵管理部22は、XML文書に電子署名を行うために用いる秘密鍵を管理する。また、電子署名を行うために用意された秘密鍵に対し、当該鍵を取得するための取得条件（使用条件）を設定し、これを管理することもできる。すなわち、秘密鍵を用いる上で時間や前提となる処理などの取得条件を設定した場合、設定された取得条件を満足したならば、対応する秘密鍵を使用可能とし、それ以外の場合には当該秘密鍵を使用不可能とする。秘密鍵の使用の可否は、例えば、当該秘密鍵のデータをロードしたりアンロードしたりすることにより制御できる。例えば、所定の電子署名に関して、一日のうちで一定の時間帯にのみ署名を行うことができるという時間的条件を設定した場合、当該時間帯にのみ当該電子署名の生成に必要な秘密鍵をロードして使用できるようにする。このように取得条件を設定すれば、秘密鍵を取得するために一定の条件を満足することが必要となるため、当該秘密鍵を用いてなされた電子署名の信頼性を高めることができる。

【0036】署名鍵取得部23は、署名鍵判定部21によりXML文書の内容に応じて選択された秘密鍵を鍵管理部22から取得し、署名生成部24に渡す。上述したように、秘密鍵に取得条件が設定されている場合であって、署名鍵判定部21が秘密鍵を選択した時点では当該秘密鍵の取得条件を満足していない場合、デフォルトで設定されている代替の秘密鍵（以下、代替鍵と称す）を署名生成部24に渡すことができる。この場合、署名鍵判定部21により選択された秘密鍵の取得条件を満足した時点で、当該秘密鍵を改めて取得し、署名生成部24に渡すようにすることもできる。上述した時間的制約を

取得条件として設定した場合、署名鍵取得部２３が秘密鍵を取得しようとした時が、当該秘密鍵が鍵管理部２２にロードされている時間帯でない場合、署名鍵取得部２３は、代替鍵を署名生成部２４に渡しておく。そして、当該秘密鍵が鍵管理部２２にロードされる時間帯になったならば、署名鍵取得部２３は、当該秘密鍵を鍵管理部２２から取得し、署名生成部２４に渡す。

【００３７】署名生成部２４は、ＸＭＬ文書に対して、署名鍵取得部２３により取得された秘密鍵を用いて電子署名を行う。電子署名を行う対象のＸＭＬ文書は、原則的には、アプリケーション１０から送信され、スイッチ３０にてインターセプトして取得されたＸＭＬ文書である。しかし、上記のように、秘密鍵に対して取得条件が設定されている場合であって、インターセプトにより取得したＸＭＬ文書に対して代替鍵を用いて電子署名を行っていた場合は、当該ＸＭＬ文書に対して、本来の秘密鍵を取得した後に改めて当該秘密鍵を用いて電子署名を行う。この場合、当該秘密鍵を用いた事後的な電子署名は、代替鍵を用いた電子署名を施されたＸＭＬ文書に追加的に行っても良いし、代替鍵を用いた電子署名を施す前の状態のＸＭＬ文書に改めて新規に行っても良い。署名生成部２４により電子署名を施されたＸＭＬ文書は、ＬＡＮ１００に戻されてアプリケーション１０から送信された際の送信先に送られると共に、ログ管理部２５に送られ、管理される。

【００３８】ログ管理部２５は、署名生成部２４により電子署名を施したＸＭＬ文書のログを取り、管理する。電子署名の施されたＸＭＬ文書は、通常、後の監査のために安全に格納されなければならない。ログはアプリケーション１０や通信のレベルでも取ることができるが、有効な署名をもったログを取るには、署名時あるいは検証時に取ることが最適である。少なくともログを取った段階では署名が正しいことが保証されているからである。署名時にログを取らないと、何に対して署名したのか、後で監査できない事態も起こり得る。署名の付いたＸＭＬ文書のログをとるには、署名生成部２４により署名されたＸＭＬ文書を、そのまま長期安定記憶装置（ハードディスクなど）に格納すれば良い。格納されたＸＭＬ文書には電子署名が付加されているので、ログの不正な改ざんがなされることはない。なお、ログには、例えばクレジットカード番号などの機密性の高い情報が入っている可能性がある。このため、ログのアクセスには、適当なアクセス制限をつける必要がある。このアクセスコントロールは、ログの一部分（例えばクレジットカード番号だけ）に適用することもできる。また、上述したように、秘密鍵の取得に取得条件を設定した場合、後に代替鍵を用いて署名されたＸＭＬ文書に対して当該秘密鍵を用いて改めて署名するために、電子署名の付加されていない状態のＸＭＬ文書を併せて格納し、管理しておくこともできる。

【００３９】図３は、署名プロキシサーバ２０の電子署名の検証に関する構成を示す図である。図３を参照すると、署名プロキシサーバ２０は、受信したメッセージ文書から電子署名の署名情報を取得する署名情報取得部３１と、取得された署名情報を検証するために用いる公開鍵を管理する鍵管理部３２と、取得された署名情報に基づいて電子署名の正当性を検証する検証部３３と、受信したメッセージ文書のログを管理するログ管理部３４とを備える。

【００４０】署名情報取得部３１は、社外から受信したメッセージ文書であるＸＭＬ文書を取得する。そして、当該ＸＭＬ文書に付加されている電子署名の署名情報を取得すると共に、当該ＸＭＬ文書に記載された情報に基づいて、当該ＸＭＬ文書を検証するために必要な公開鍵を鍵管理部３２から取得し、検証部３３に渡す。

【００４１】鍵管理部３２は、ＸＭＬ文書に付加されている電子署名を検証するための公開鍵を管理している。公開鍵は、予めＸＭＬ文書の署名に用いられる秘密鍵に対応した公開鍵を署名プロキシサーバ２０や企業内のネットワークシステム上に保管手段を設けて保管しても良いし、外部認証機関からネットワークを介して取得しても良い。

【００４２】検証部３３は、当該ＸＭＬ文書の内容に応じた公開鍵を用いて電子署名を検証する。そして、当該ＸＭＬ文書の正当性が確認されたならば、当該ＸＭＬ文書をＬＡＮ１００に戻して送信先であるアプリケーション１０に送ると共に、ログ管理部３４に送る。また、当該ＸＭＬ文書の正当性が否定されたならば、当該ＸＭＬ文書をＬＡＮ１００に戻すことなく、予め設定されたエラー処理を行う。ＸＭＬ文書に付加された電子署名が、当該ＸＭＬ文書の内容に応じた秘密鍵を用いて行われた電子署名ではなく、予め決められた代替鍵を用いて行われた電子署名である場合（これは、電子署名を検証する際の公開鍵を選択することによって認識できる）、検証部３３は、本来の秘密鍵を用いて署名されたＸＭＬ文書の到着を待って最終的な正当性の判断を行う。

【００４３】この場合、代替鍵を用いて署名されたＸＭＬ文書については、本来の秘密鍵を用いて署名されたＸＭＬ文書が到着するまで署名プロキシサーバ２０に留めておいても良いし、本来の秘密鍵を用いて署名されたＸＭＬ文書の到着を待たずにアプリケーション１０に送り、先行して処理を進めるようにしても良い。いずれの場合であっても、代替鍵を用いて署名されたＸＭＬ文書の有効期限を定めておき、本来の秘密鍵を用いて署名されたＸＭＬ文書が当該有効期限以内に到着しない場合は、当該代替鍵を用いて署名されたＸＭＬ文書を無効とする。なお、代替鍵を用いて署名されたＸＭＬ文書と本来の秘密鍵を用いて署名されたＸＭＬ文書とを結びつけるには、文書ＩＤを照合するなどの手段を取ることができる。

【００４４】代替鍵を用いて電子署名を行う手法を効果的に行う実施態様として、代替鍵を用いて署名されたＸＭＬ文書により処理を進めておき、予め定められた一定の時間が過ぎても本来の秘密鍵を用いて署名されたＸＭＬ文書が到着しない場合に、先行して進められた処理を無効とするような制御を行うことが考えられる。

【００４５】ログ管理部３４は、検証部３３により検証された署名付きＸＭＬ文書及びその検証結果のログを取り、管理する。署名付きＸＭＬ文書のログをとるには、検証部３３により検証されたＸＭＬ文書を、そのまま長期安定記憶装置（ハードディスクなど）に格納すれば良い。格納されたＸＭＬ文書には電子署名が付加されているので、ログの不正な改ざんがなされることはない。こうして蓄積されたログデータを、取引相手の署名プロキシサーバ２０における署名実行側のログ管理部２５に管理されているログデータと比較することにより、ログデータの完全性を保証し、業務のセキュリティをさらに強固にすることができる。

【００４６】ここで、ログデータの比較は、ログ管理部２５に蓄積されたログにおける署名付きＸＭＬ文書の全てについて行う必要はなく、電子署名の署名情報、特に署名の際に用いられるハッシュ値を比較すれば十分である。例として、図１の企業Ａ、Ｂ間のメッセージ通信におけるログデータの比較を考える。この場合、月ごとなどの一定のタイミングで、企業Ａ、Ｂ双方のログデータのうち、ハッシュ値を相互に交換し比較する。そして、企業Ａ、Ｂ間におけるメッセージ通信に用いられたハッシュ値が共通すれば、全てのメッセージ通信が電子署名により双方で認証されていることがわかる。一方、このハッシュ値が相違する場合は、企業Ａ、Ｂのいずれか一方が認証していないメッセージ通信が存在することがわかる。そこで、今度は全てのログデータを交換し、どのメッセージ文書が企業Ａ、Ｂの認証を受けていないのかを探索する。

【００４７】なお、図２、３に示した署名プロキシサーバ２０の各構成要素は、コンピュータプログラムにより制御されたＣＰＵにて実現される仮想的なソフトウェアブロックである。ＣＰＵを制御する当該コンピュータプログラムはＣＤ－ＲＯＭやフロッピー（登録商標）ディスクなどの記憶媒体に格納したり、ネットワークを介して伝送したりすることにより提供される。また、上記の説明では、図２及び図３は、同一の署名プロキシサーバ２０における電子署名の付加に関する構成と、電子署名の検証に関する構成とをそれぞれ示すこととしたが、図２に示すプロキシサーバと、図３に示すプロキシサーバとを別々に構成しても良い。

【００４８】次に、図２に示した署名プロキシサーバ２０の鍵管理部２２、署名鍵取得部２３、署名生成部２４及びログ管理部２５により実現される事後署名の動作について説明する。図４は、本来の秘密鍵を使用できない場合を含む署名動作を説明するフローチャートである。図４を参照すると、まず、署名鍵取得部２３が、署名鍵判定部２１により選択された秘密鍵が使用可能かどうかを鍵管理部２２に問い合わせる（ステップ４０１）。当該秘密鍵が使用可能であれば、当該秘密鍵を取得して署名生成部２４に渡す。署名生成部２４は、当該秘密鍵を用いて署名を行い、電子署名付きＸＭＬ文書を送信して処理を終了する（ステップ４０２）。

【００４９】一方、当該秘密鍵の取得条件が満たされておらず使用できない場合、署名鍵取得部２３は、デフォルトの代替鍵を鍵管理部２２から取得して署名生成部２４に渡す。署名生成部２４は、当該代替鍵を用いて署名を行い、電子署名付きＸＭＬ文書を送信する（ステップ４０３）。そして、ログ管理部２５が、事後署名の対象用に用意されたログ（事後署名用ログ）に当該ＸＭＬ文書を書き込む（ステップ４０４）。ここで、事後的に行う本来の秘密鍵による署名を代替鍵により署名されたＸＭＬ文書に対して追加的に行う場合は、事後署名用ログに、代替鍵を用いて署名されたＸＭＬ文書を格納する。また、本来の秘密鍵による署名を代替鍵により署名される前の状態のＸＭＬ文書に対して新規に行う場合は、事後署名用ログに、署名されていないＸＭＬ文書を格納する。

【００５０】図５は、鍵管理部２２において、所定の秘密鍵の取得条件が満たされ、使用可能となった場合の動作を説明するフローチャートである。図５を参照すると、所定の秘密鍵が使用可能になった場合、ログ管理部２５は、当該秘密鍵で事後署名を行う必要のあるＸＭＬ文書が存在するかチェックする（ステップ５０１、５０２）。そして、そのようなＸＭＬ文書が事後署名用ログに存在するならば、署名生成部２４が、署名鍵取得部２３を介して当該秘密鍵を受け取り、ログ管理部２５から該当するＸＭＬ文書を受け取って署名を行い、電子署名付きＸＭＬ文書を送信する（ステップ５０３、５０４）。

【００５１】以上のようにして、必要な秘密鍵が使用できない場合に代替鍵による署名を行った文書を送信し（図４）、当該秘密鍵が使用可能となった場合に事後的に当該秘密鍵による署名を行った文書を送信する（図５）。

【００５２】なお、電子署名には一意な連続番号が振られるものとする。このようにすれば、上記のような事後署名や、処理上の誤りによって同じメッセージ文書を２度送信してしまったとしても、当該メッセージ文書に基づく作業（例えば、メッセージ文書による発注に対する受注処理など）を重複して行ってしまうことを防止することができる。

【００５３】

【発明の効果】以上説明したように、本発明によれば、ネットワークを介して送受されるメッセージの電子署

名、検証、ロギングを行う手段をプロキシサーバの形で実装することにより、アプリケーション・プログラムの変更を必要とせずに、電子署名によるセキュリティ機能を実現することができる。

【００５４】また、本発明によれば、プロキシサーバを用いて電子署名及び検証を制御することにより、事後署名のような署名方法を実現することができる。

【００５５】さらにまた、本発明によれば、プロキシサーバを用いてメッセージのロギングを行うことにより、メッセージのログに対するアクセス制御を可能とすることができる。

【図面の簡単な説明】

【図１】　本実施の形態における電子署名システムの全体構成を説明する図である。

【図２】　本実施の形態における署名プロキシサーバの電子署名の付加に関する構成を示す図である。

【図３】　本実施の形態における署名プロキシサーバの電子署名の検証に関する構成を示す図である。

【図４】　本来の秘密鍵を使用できない場合を含む署名動作を説明するフローチャートである。

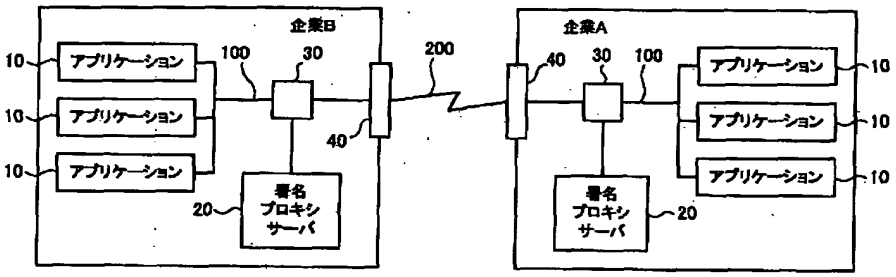
【図５】　秘密鍵の取得条件が満たされて使用可能となった場合の署名動作を説明するフローチャートである。

【図６】　ＸＭＬ形式で記述された鍵選択ルールの例を示す図である。

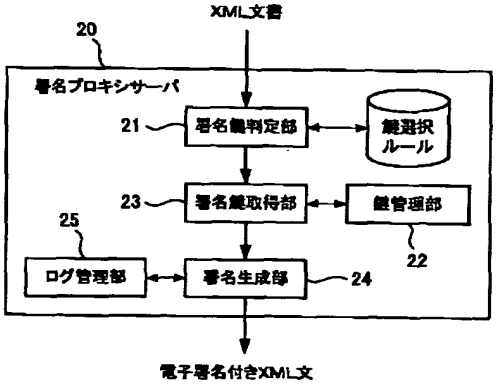
【符号の説明】

１０…アプリケーション、２０…署名プロキシサーバ、２１…署名鍵判定部、２２…鍵管理部、２３…署名鍵取得部、２４…署名生成部、２５…ログ管理部、３０…スイッチ、４０…ファイヤーウォール、１００…ＬＡＮ、２００…ネットワーク

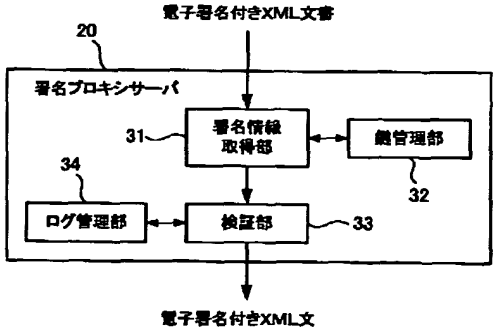
【図１】



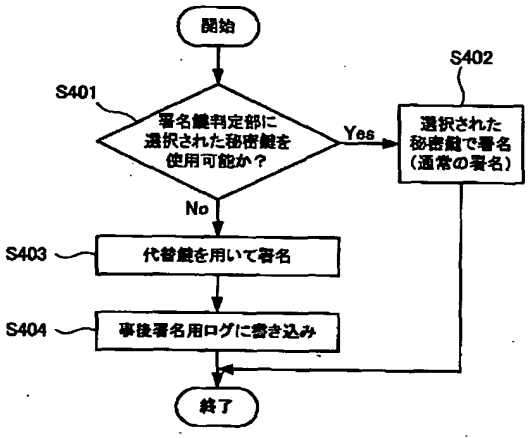

【図２】



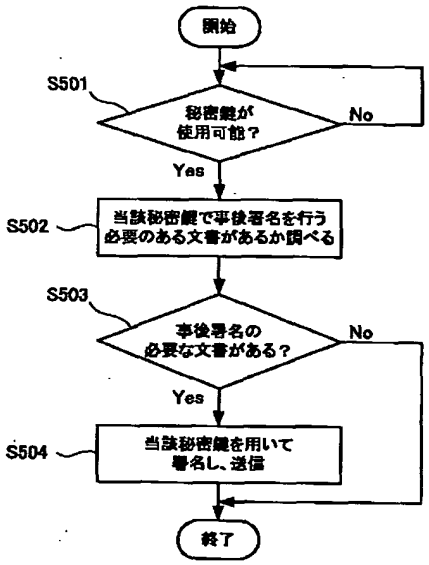

【図３】



【図4】




【図5】




【図6】

```
<rule>

  <!— root要素がpurchaseOrderで、level属性が"A"(100万円以上)の時は、会社の鍵を使う —>

  <description about="//purcheOrder[@level='A']">

     <key ID="SigningKeyForCompany">

     <— 到着したら、確認のためにメールを出す —>
     <whenArrived>
        <confirm mail="ohtoshi@jp.ibm.com">
     </whenArrived>

  </decription>

  <!— root要素がpurchaseOrderで、level属性が"B"(10万円以上)の時は、担当者の鍵を使う —>
  <description about="//purcheOrder[@level='B']">
     <key ID="SigningKeyForManager">
  </decription>

  ...

</rule>
```

---

フロントページの続き

(72)発明者　丸山　宏
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

(72)発明者　浦本　直彦
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Fターム(参考) 5J104 AA09 AA16 EA04 EA16 EA25
JA21 LA03 LA05 LA06 MA02
MA06 NA02 PA07 PA10